BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Pada penelitian sebelumnya yang dilakukan oleh Dwi Kuswanto dalam jurnal yang berjudul "Unjuk Kerja Intrusion Prevention Sistem (IPS) Berbasis Suricata Pada Jaringan Lokal Area *Network* Laboratorium TIA Teknik Informatika Universitas Trunojoyo. Pada penelitian ini, pendeteksi serangan yang digunakan adalah suricata. Penelitian ini ditujukan untuk mengimplementasikan Intrusion Prevention System (IPS) berbasis Suricata dengan mengkombinasikan IPTables pada jaringan komputer LAN. Dan pada penelitian ini, monitoring dilakukan keamanan jaringan dilakukan melalui *web*. *WebAdmin* memudahkan seorang Administrator jaringan dengan bantuan peringatan jika ada serangan dan dapat mengamati statistik serangan dan keadaan komputer IPS.

Pada penelitian sebelumnya yang dilakukan oleh Yudhi Arta, Abdul Syukur dan Roni Kharisma dalam jurnal yang berjudul "Simulasi Implementasi *Intrusion Prevention System* (IPS) Pada *Router MikroTik*". Pada penelitian ini rules IPS dikonfigurasi pada *router MikroTik*. Serangan terdeteksi tergantung pada pola serangan yang ada di dalam *rules* IPS tersebut. Untuk itu pengolaan filter *rules* pada perangkat IPS harus secara rutin melakukan pengembangan *rules*. Pada penelitian ini, monitoring serangan dilakukan melalui log mikrotik tanpa tambahan aplikasi monitoring lainnya.

Pada penelitian sebelumnya yang dilakukan oleh Abdul Muhaimi dalam jurnal yang berjudul "Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terinegrasi Dengan Telegram". Penelitian ini menggunakan snort sebagai pendeteksi dan pemblokiran dengan *IPTables* yang dikemas dalam bentuk *shell script* dan dipicu eksekusinya oleh aplikasi IM *Auto Reply* ketikan serangan tersebut terjadi sehingga meminimalkan

campur tangan secara manual dari *administrator*. Penelitian ini menggunakan *telegram* untuk memonitoring penyerangan yang terjadi.

Berdasarkan penelitian sebelumnya, maka mendorong penulis untuk mengaplikasikan *rules* IPS berdasarkan jenis serangan pada *MikroTik* dengan notifikasi berbasis telegram yang mempermudah administrator untuk memantau serangan yang terjadi. Dengan adanya *rules* IPS yang telah dikonfigurasi pada *MikroTik* maka IP penyerang tersebut akan diblokir dan tidak bisa melakukan jenis penyerangan yang sama kepada target. Dengan adanya notifikasi *telegram* penyerangan ini, administrator tidak perlu lagi memantau keamanan server selaman 24 jam karna setiap akan terjadi serangan maka ada notifikasi secara langsung lewat *telegram* untuk mengetahui kondisi system yang dapat diketahui jenis serangan yang dilakukan oleh *attacker*. *Administrator* juga tidak perlu melakukan tindakan lebih karna otomatis serangan akan dicegah menggunakan metode IPS.

2.2 Jaringan Komputer

Menurut Sofana (2013 : 3), jaringan komputer adalah suatu himpunan yang terkoneksi sejumlah komputer *autonomous*. Dalam bahasa yang popoler dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (*nirkabel*). Informasi berupa data akan mengalir dari satu komputer ke perangkat yang lain, sehingga masingmasing komputer yang terhubung tersebut bisa saling bertukar data atau berbagi perangkat keras.

2.3 Jenis-jenis Jaringan Komputer

Berdasarkan Jangkauan area atau lokasi, jaringan di bedakan menjadi beberapa jenis yaitu:

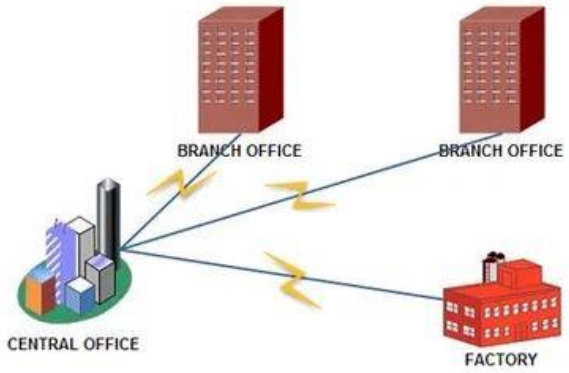
1. Personal Area Network (PAN)

Menurut MADCOM (2015:3) *Personal Area Network* (PAN) yaitu saat anda menghubungkan komputer keperangkat lain seperti *handphone, personal digital assitant, keyboard, mouse, headset wireless,* kamera dan peralatan lain yang jarak nya cukup dekat sekita 4-6 meter, maka anda telah membentuk suatu sistem jaringan pribadi atau *Personal Area Network* (PAN). Dalam hal ini yang paling penting adalahyang mengendalikan (*authority*) pada peralatan tersebut. *Personal Area Network* (PAN) juga sering dibentuk di teknologi *wireless* atau nirkabel seperti *bluetooth ,infrared atau wifi*.

Gambar 2.1 PAN (*Personal Area Network*)
(Sumber: Wongkar, 2015)

2. Metropolitan Area Network (MAN)

Menurut Sofana (2009:112) "*Metropolitan Area Network* (MAN) merupakan jaringan komputer yang meliputi area seukuran kota atau gabungan beberapa *Local Area Network* (LAN) yang dihubungkan menjadi sebuah jaringan besar, *Metropolitan Area Network* (MAN) dapat memanfaatkan jaringan TV kabel yang umumnya menggunakan kabel *coaxsial* atau serat optik".

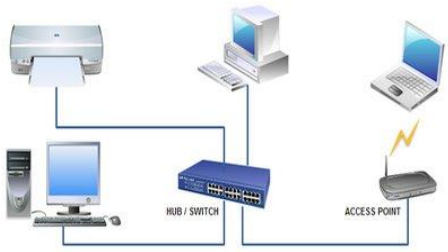


Gambar 2.2 MAN (*Metropolitan Area Network*)

(Sumber: Wongkar, 2015)

3. Local Area Network (LAN)

Menurut Sofana (2009:113) "LAN (*Local Area Network*) beberapa buah PC dapat membentuk network, berhubungan dengan area network yang berukuran relatif kecil. Oleh karena itu, LAN (*Local Area Network*) dapat dikembangkandengan mudah dan mendukung kecepatan transfer data cukup tinggi".

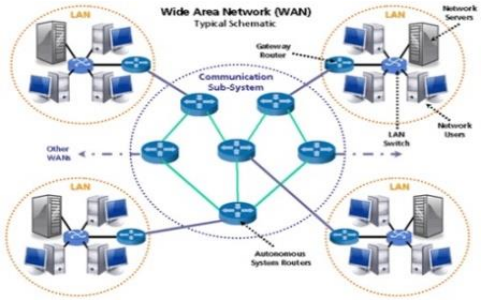


Gambar 2.3 LAN (*Local Area Network*)
(Sumber: Wongkar, 2015)

4. Wide Area Network (WAN)

Menurut Sofana (2009:127) "WAN (*Wide Area Network*) memahami seluk beluk sebuah LAN(Local Area Network)merupakan langkah awal untuk memahami teknologi jaringan secara umum". Manakala LAN (*Local Area Network*) dihubungkan dengan media komunikasi publik atau lainnya, seperti jaringan telepon

dan melibatkan area geografis yang cukup besar, Seperti antarnegara antarbenua, maka model jaringan berskala besat disebut WAN (*Wide Area Network*).



Gambar 2.4 WAN (*Wide Area Network*)
(Sumber: Wongkar, 2015)

5. Internet

Menurut Sofana (2013:5) "*Internet* adalah interkoneksi jaringan komputer skala besar (mirip WAN), yang dihubungkan menggunakan protokol khusus. Jadi sebenarnya *Internet*merupakan bagian dari WAN(Wide Area Netwrok)". Cakupan *Internet*adalah satu dunia bahkan tidak menutup kemungkinan antarplanet. Koneksi antarjaringan komputer dapat dilakukan berkat dukungan prokotol khas, yaitu TCP/IP(Transmission Control *Protocol* / *Internet Protocol*).

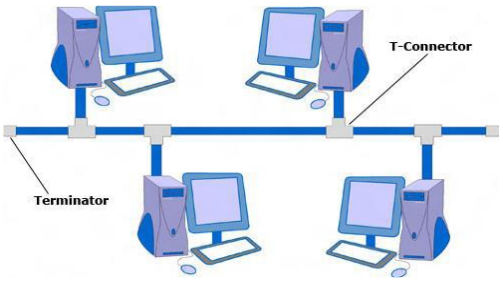
2.4 Topologi Jaringan

Menurut Arifin (2011:29) menyatakan bahwa "Jaringan komputer terbentuk dari beberapa komputer yang saling terhubung melalui media komunikasi (kabel/nirkabel) dan beberapa perangkat keras pendukungnya. Cara menghubungkan komputer satu dengan yang lainnya sehingga membentuk jaringan disebut Topologi."

2.4.1. Topologi Jaringan Bus

Menurut Sofana (2013:10) " Topologi busSering juga disebut *daisy chain* atau ethernet bus *topologies*. Jaringan yang menggunakan topologi bus dapat dikenali dari penggunaan kabel backbone (kabel utama) yang menghubungkan semua peralatan jaringan (device). Karena kabel backbone menjadi satu-satunya jalan bagi lalu lintas

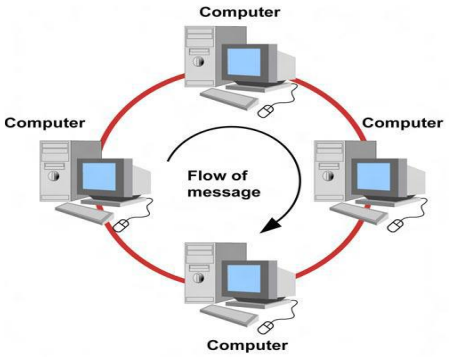
data maka apabila kabel backbone rusak atau terputus akan menyebabkan jaringan terputus total.



Gambar 2.5 Topologi *Bus*
(Sumber: Ginta, 2015)

2.4.2 Topologi Jaringan Ring

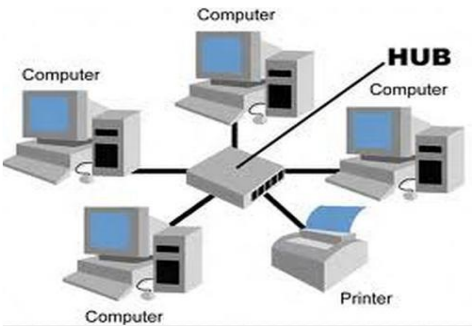
Menurut Sofana (2013:22) "Topologi ring sangat berbeda dengan Topologi bus. Setiap komputer terhubung dengan kabel *backbone*. Setelah sampai pada komputer terakhir maka ujung kabel akan kembali dihubungkan dengan komputer pertama".



Gambar 2.6 Topologi *Ring*
(Sumber: Ginta, 2013)

2.4.3 Topologi Jaringan Star

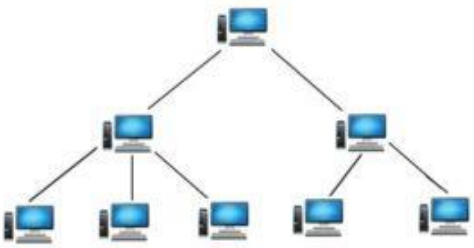
Menurut Sofana (2013:33) "Topologi star dikenali dengan keberadaan sebuah sentral berupa hub yang menghubungkan semua node. Setiap *node* menggunakan sebuah kabel UTP (*Unshielded Twisted Pair*) atau STP (*Shielded Twisted Pair*) yang di hubungkan melalui *ethernet card* ke *hub*.



Gambar 2.7 Topologi *Star*
(Sumber: Ginta, 2013)

2.4.4 Topologi Jaringan Tree

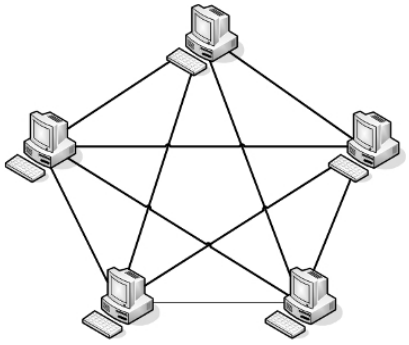
Menurut Sofana (2013:54) "Topologi tree disebut juga topologi star-bus atau star/bus hybrid. Topologi tree merupakan gabungan beberapa topologi star yang dihubungkan dengan topologi bus. Topologi tree digunakan untuk menghubungkan beberapa LAN(Local Area Network)dengan LAN *(Local Area Network)* lain". Hubungan antar-LAN dilakukan via hub. Masing-masing pohon (tree).



Gambar 2.8 Topologi Tree
(Sumber: Ginta, 2013)

2.4.5 Topologi Jaringan Mesh

Menurut Sofana (2013:55) "Topologi mesh dapat dikenali dengan hubungan point to point atau satu-satu ke setiap komputer. Setiap Komputer terhubung ke komputer lain melalui kabel, bisa menggunakan kabel *coaxsial, twisted pair*, bahkan serat optik". Topologi mesh cocok digunakan pada jaringan yang sangat kritis.



Gambar 2.9 Topologi *Mesh*

(Sumber: Ginta, 2013)

2.5 Intrusion Prevention Sistem (IPS)

Intrusion Prevention Sistem adalah sebuah aplikasi yang bekerja untuk mendeteksi aktivitas mencurigakan, dan melakukan pencegahan terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti bagaimana mestinnya (Monoarfa, M., dkk 2016).

Secara konsep, IPS adalah sistem yang mampu atau memiliki fungsi mendeteksi dan memberikan penanganan serangan. Dengan kata lain, IPS merupakan pengembangan dari IDS dengan menambahkan beberapa komponen seperti firewall dan beberapa komponen lain untuk bekerja sama dalam mencegah dan menghentikan terjadinya penyusupan dari client (Rudy Suwanto, 2019).

IPS (*Intrusion Prevention System*) merupakan sebuah perangkat lunak yang beroperasi untuk mengidentifikasi dan memblokir ancaman terhadap jaringan dengan menilai setiap paket yang melintasi berdasarkan protokol jaringan pada aplikasi dan kemudian melakukan pelacakan ancaman keamanan jaringan. Sistem IPS sama dengan sistem setup IDS, IPS mampu mencegah beberapa ancaman yang datang dengan sedikit bantuan administrator atau bahkan tidak sama sekali.

Serangan biasanya datang dalam bentuk input data berbahaya ke aplikasi target atau melalui layanan yang digunakan penyerang untuk mengganggu dan menguasai aplikasi atau jaringan target. Oleh karena itu IPS akan melakukan suatu

tindakan untuk mencegah serangan sebelum terjadi eksekusi dalam memori dan IPS akan membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga menginterupsi sistem panggilan.

Secara khusus, IPS memiliki empat komponen utama, yaitu:

1. *Normalisasi Traffic* : menginterpretasikan *traffic* jaringan dan melakukan analisa terhadap paket yang disusun kembali, seperti halnya fungsi block sederhana.
2. *Detection Engine* : mendeteksi *traffic* jaringan dan melakukan patternmatchingterhadap tabel acuan dan respon yang sesuai.
3. *Service Scanner* : membangun suatu tabel acuan untuk mengelompokkan informasi.
4. *Traffic Shaper* : membentuk dan mengatur *traffic* jaringan.

2.5.1 Host Based IPS (HIPS)

Host-based Intrusion Prevention Sistem (HIPS) sama seperti halnya *Host Based Intrusion Detection Sistem* (HIDS). *Program agent* HIPS diinstall secara langsung di sistem yang diproteksi untuk dimonitor aktifitas sistem internalnya. HIPS di binding dengan kernel sistem operasi dan services sistem operasi sehingga HIPS bisa memantau dan menghadang sistem call yang dicurigai dalam rangka mencegah terjadinya intrusi terhadap host. HIPS juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu. Sebagai contoh HIPS untuk mencegah intrusion pada webserver misalnya. Dari sisi security mungkin solusi HIPS bisa mencegah datangnya ancaman terhadap host. Tetapi dari sisi *performance*, harus diperhatikan apakah HIPS memberikan dampak negative terhadap performance host. Karena menginstall dan binding HIPS pada sistem operasi mengakibatkan penggunaan *resource* komputer host menjadi semakin besar (Yoga Widya, 2017).

2.5.2 Network Based IPS (NIPS)

Network-based Intrusion Prevention Sistem (NIPS) tidak melakukanpantauan secara khusus di satu host saja. Tetapi melakukan pantauan dan proteksi II-16 dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan *firewall* dan

kadang disebut sebagai *In-Line* IDS atau *Gateway Intrusion Detection Sistem* (GIDS). Sistem kerja IPS yang populer yaitu pendeteksian berbasis signature, pendeteksian berbasis anomali, dan monitoring file pada sistem operasi host. (Yoga Widya, 2017)

a. Sistematika IPS yang berbasis signature adalah dengan cara mencocokkan lalu lintas jaringan dengan signature database milik IPS yang berisi attacking rule atau cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama halnya dengan antivirus, IPS berbasis *signature* membutuhkan *update* terhadap *signature database* untuk metodemetode penyerangan terbaru. IPS berbasis *signature* juga melakukan pencegahan terhadap ancaman intrusi sesuai dengan *signature database* yang bersangkutan.
b. Sistematika IPS yang berbasis anomali adalah dengan cara melibatkan pola-pola lalu lintas jaringan yang pernah terjadi. Umumnya, dilakukan dengan menggunakan teknik statistik. Statistik tersebut mencakup perbandingan antara lalu lintas jaringan yang sedang di monitor dengan lalu lintas jaringan yang biasa terjadi (*normal state*). Metode ini dapat dikatakan lebih kaya dibandingkan signature-based IPS. Karena anomalybased IPS dapat mendeteksi gangguan terhadap jaringan yang terbaru yang belum terdapat di database IPS. Tetapi kelemahannya adalah potensi timbulnya *false positive*, yaitu pesan/log yang belum semestinya dilaporkan. Sehingga tugas Network *Administrator* menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan false positive yang muncul. Teknik lain yang digunakan adalah dengan cara melakukan monitoring berkas-berkas sistem operasi pada host. IPS akan melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini diimplementasikan dalam IPS jenis Host Based Intrusion Prevention Sistem (HIPS). Teknik yang digunakan IPS untuk mencegah serangan ada dua, yaitu sniping dan shunning.

a. *Sniping*: memungkinkan IPS untuk menterminasi serangan yang dicurigai melalui penggunaan paket TCP RST atau pesan ICMP *Unreachable*.
b. *Shunning*: memungkinkan IPS mengkonfigurasi secara otomatis *firewall* untuk melakukan *drop traffic* berdasarkan apa yang dideteksi oleh IPS. Untuk kemudian melakukan prevention atau pencegahan terhadap koneksi tertentu.

2.6 Firewall

Firewall adalah sebuah sistem atau perangkat yang bertugas untuk mengatur lalu lintas jaringan komputer yang dianggap aman untuk melewatinya dan mencegah lalu lintas jaringan yang dianggap tidak aman untuk melewatinya. (Athailah, 2013). Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy*) dari organisasi. Hal ini dapat dibagi menjadi dua bagian:

1. Apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohibited*).
2. Apa yang tidak dilarang secara eksplisit dianggap diperbolehkan (*permitted*).

Firewall bekerja dengan mengamati packet IP (*Internet Protocol*) yang melewatinya. Berdasarkan konligurasi dari firewall maka akses dapat diatur berdasarkan IP *address*, *port*, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing firewall. Untukm memahami bagaimana *firewalls* bekerja, pengesahan pertama paling sederhana memeriksa prosedur penggunaan IP alamat sebagai suatu index. IP alamat *index* identifikasi *universal* pada *internet*, baik alamat statis maupun alamat yang dinamis.

IP alamat statis adalah adalamat permanen yang merupakan alamat dari suatu mesin yang selalu dihubungkan ke *internet*. Ada banya kelas dari alamat IP statis. Satu kelas yang dapat ditemukan dengan *query*, kelas ini mesin tertinggi yang terhubung dengan jaringan, seperti domain dari *server*, *web server*, dan *root*-level mesin. Yang sudah terdaftar sebagai *hostnames* pada databaseInterNIC. Kelas yang lain dari alamat IP statis adalah alamat yang ditugaskan kedua dan ketiga dari level

mesin di dalam jaringan yang dikuasai oleh domain yang disebut *server, root server*, dan lainnya.

2.7 Router

Router adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau *internet* menuju sasarannya melalui sebuah proses yang dikenal sebagai *routing*. *Router* berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan kejaringan lainnya. *Router* bertugas untuk menyampaikan paket data dari satu jaringan ke jaringan lainnya, jaringan pengirim hanya tahu bahwa tujuan jauh dari *router*. Selain itu, *router* juga memilih jalur untuk mencapai tujuan (Cartealy,2013).

Gambar 2.10 *Router*

(Sumber: Handriyanto, 2009)

2.7.1 Jenis router

Menurut (Cartealy,2013) *Router* dipasaran terbagi menjadi tiga yaitu :

a. *Router* PC merupakan komputer dengan sistem operasi yang memiliki fasilitas untuk membagi dan men-sharing IP address, dimana perangkat (PC) yang terhubung ke komputer tersebut akan dapat menikmati IP Address atau koneksi yang disebarkan oleh sistem operasi tersebut.

b. *Router* Aplikasi merupakan suatu aplikasi yang dapat diinstal pada sistem operasi dimana memiliki kemampuan seperti *router*.
c. *Router* Hardware merupakan hardware yang memiliki kemampuan seperti *router* dari berbagai hardware yang memancarkan atau membagi IP address dan men-sharing IP address.

2.7.2 Fungsi *Router*

a. Membaca alamat logika / ip *address* source & *destination* untuk menentukan *routing* dari suatu LAN ke LAN lainnya.
b. Menyimpan *routing table* untuk menentukan rute terbaik antara LAN ke WAN.
c. Perangkat di layer 3 OSI Layer.
d. Bisa berupa "*box*" atau sebuah OS yang menjalankan sebuah daemon *routing*.
e. *Interfaces Ethernet*, Serial, ISDN BRI.

2.8 Mikrotik RouterOS

*MikroTik Router*OS merupakan sistem operasi *Linux base* yang diperuntukkan sebagai *network router*. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui *Windows Application* (*Winbox*). Selain itu instalasi dapat dilakukan pada Standard komputer PC (*Personal Computer*). PC yang akan dijadikan *router MikroTik* pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standard, misalnya hanya sebagai *gateway*. Untuk keperluan beban yang besar (*network* yang kompleks, *routing* yang rumit) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai (Handriyanto, 2009).

2.8.1 Fitur-Fitur Mikrotik

a. *AddressList* : Pengelompokan IP *Address* berdasarkan nama
b. Asynchronous : Mendukung serial PPP *dial-in* / *dial-out*, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, *Radius*, *dial on demand*, *modem pool* hingga 128 ports.

c. *Bonding* : Mendukung dalam pengkombinasian beberapa antarmuka *ethernet* ke dalam 1 pipa pada koneksi cepat.
d. *Data Rate Management* : QoS berbasis HTB dengan penggunaan *burst*, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar *peer to peer.*
e. DHCP : Mendukung DHCP tiap antarmuka; DHCP *Relay*; DHCP Client, *multiplenetwork* DHCP; *staticand dynamic* DHCP *leases.*
f. *Firewall* dan NAT : Mendukung pemfilteran koneksi *peer to peer*, *source NAT* dan *destination* NAT. Mampu memfilter berdasarkan MAC, IP *address*, *range port*, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
g. Hotspot : Hotspot *gateway* dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
h. IPSec : Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5.
i. ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui *line* protokol.
j. M3P : *MikroTik* Protokol Paket *Packer* untuk *wireless* links dan *ethernet*.
k. MNDP : *MikroTik Discovery Neighbour Protocol*, juga mendukung *Cisco Discovery Protokol* (CDP).
l. *Monitoring* / *Accounting* : Laporan *Traffic* IP, log, statistik *graph* yang dapat diakses melalui HTTP.
m. NTP : *Network* Time Protokol untuk server dan *clients*; sinkronisasi menggunakan sistem GPS.
n. *Poin to Point Tunneling Protocol* : PPTP, PPPoE dan L2TP *Access Consentrator*; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit data rate.

o. *Proxy* : *Cache* untuk FTP dan HTTP *proxy* server, HTTPS *proxy*; transparent *proxy* untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent *proxy*; static DNS.
p. *Routing* : *Routing* statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
q. SDSL : Mendukung *Single Line* DSL; mode pemutusan jalur koneksi dan jaringan.
r. *SimpleTunnel* : *Tunnel* IPIP dan EoIP (*Ethernet* over IP).
s. SNMP : *SimpleNetworkMonitoring Protocol* mode akses *read-only*.
t. Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media *types*; sync-PPP, Cisco HDLC; *Frame Relay* line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); *FrameRelay* jenis LMI.
u. Tool : Ping, *Traceroute*; *bandwidth test*; ping flood; telnet; SSH; *packetsniffer*; Dinamik DNS *update*.
v. UPnP : Mendukung antarmuka *Universal Plug and Play*.
w. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan *ethernet* dan *wireless*; multiple VLAN; VLAN bridging.
x. VoIP : Mendukung aplikasi *voice over* IP.
y. VRRP : Mendukung *Virtual Router Redudant Protocol*.
z. *Winbox* : Aplikasi mode GUI untuk meremote dan mengkonfigurasi *MikroTik Router*OS.

Gambar 2.11 *MikroTik*
(Sumber**:***www.mikrotik.com)*

2.9 Aplikasi Winbox

Winbox adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke *serve*r *MikroTik* dalam mode *GUI*. Mengkonfigurasi *MikroTik* melaui *winbox* ini lebih banyak digunakan karena selain penggunaannya yang mudah, juga tidak harus menghapal perintah-perintah *console* (Muhammad, 2017).

2.9.1 Fungsi *Winbox*

Fungsi utama *winbox* adalah untuk *setting* yang ada pada *MikroTik*, berarti tugas utama *winbox* adalah untuk men*setting* atau mengatur *MikroTik* dengan GUI, fungsi *winbox* lebih rinci adalah untuk melakukan setting *MikroTik router*, untuk setting *bandwidth* jaringan *internet*, dan untuk *setting* blokir sebuah situs (Didi, 2016).

2.10 Jenis Serangan pada Jaringan Komputer

2.10.1 Port Scanning (Nmap)

Port scanning merupakan langkah awal serangan terhadap jaringan komputer. Dari keberhasilan melakukan *port scanning*, penyerang dapat melanjutkan serangan lanjutan ke jaringan komputer. Penyerangan *port scanning* dapat dilakukan dengan *Nmap. Nmap (Network Mapper)* merupakan sebuah alat untuk eksplorasi dan audit keamanan jaringan. Dengan menggunakan alat ini, dapat melihat *host* yang aktif, *port* yang terbuka, sistem operasi yang digunakan dan fungsi – fungsi *scanning* lainnya. (Huda, 2020).

2.10.2 Telnet Brute Force

Telnet merupakan kependekan *Telecommunication Network*, yang memungkinkan sebuah jaringan atau koneksi jaringan dibangun (*established)* secara *remote. Telnet* merupakan suatu protokol yang memungkinkan penggunanya dapat *login* dan bekerja pada sistem jarak jauh, seperti jika terdapat program maupun *file* yang tersimpan pada komputer jarak jauh tersebut berada di komputer pengguna.

Singkatnya, *Telnet* merupakan *software* yang digunakan untuk melakukan control jarak jauh pada sistem komputer. (Wardana, 2019).

2.10.3 SSH Brute Force

SSH (*Secure Shell*) adalah protokol yang digunakan untuk megendalikan komputer dari jarak jauh untuk mengirim *file*, membuat tunnel yang terenkripsi, dan lainnya. (Suprapto, 2018).

2.10.4 FTP Brute Force

FTP (File Transfer Protocol) adalah suatu *protocol* yang berfungsi untuk tukar – menukar file dalam suatu *network* yang men-*support* TCP/IP *protocol*. Dua hal penting yang ada dalam FTP adalah FTP *server* dan FTP *client*. FTP *server* menjalankan *software* yang digunakan untuk tukar – menukar *file*, yang selalu siap memberikan layanan FTP apabila mendapat *request* dari FTP *client*. FTP *client* adalah komputer yang me-*request* koneksi ke FTP *server* untuk tujuan tukar menukar *file* (meng-*upload* atau men-*download file*). FTP sebenarnya cara yang tidak aman untuk men-*transfer file* karena *file* tersebut di-*transfer* tanpa melalui enkripsi terlebih dahulu tetapi melalui *clear text.* (Ryan, 2018).

2.11 Perl

Perl adalah bahasa pemrograman yang dikembangkan oleh Lerry Well yang khusus dirancang untuk perencanaan teks. Perl sendiri adalah sebuah akronim, yaitu singkatan dari Practical Extracton adan Regart Language. Saat ini Per dapat berjalan di berbagai platform, seperti Windows, Mac OS, dan berbagai versi UNIX. Perl diciptakan dengan menggabungkan unsur-unsur dari bahasa *C, awk, Bourne shell script, dan program-program seperti sed, grep*. Tidak seperti shell script, Perl tidak bergantung pada program-program eksternal, sehingga lebih cepat. Perl merupakan setengah kompiler juga setengah interpreter. Jika kita menjalankan sebuah skrip Perl, maka skrip tersebut sebenarnya dikompilasi terlebih dahulu ke dalam bentuk menengah (*pohon syntax*) yang kemudian di interpretasikan oleh sistem run-time

Perl. Dengan demikian, eksekusi skrip Perl lebih cepat daripada skrip bahasa-bahasa yang murni terinterpretasi (*interpreted language*) seperti Tcl. (Jubilee, 2017).

2.12 Telegram

Telegram adalah layanan pesan populer yang berbasis pada platform *open-source* yang dibangun oleh Rusia Pavel Durov pada tahun 2013. *Telegram* merupakan aplikasi cloud based dan sistem enkripsi yang menyediakan enkripsi *end-to-end, self destruction messages*, dan infrastruktur *multidata center*. Kemuadahan akses yang diberikan telegram yang dapat berjalan di hampir semua platform memberikan kemudahan bagi *administrator* untuk membangun sistem notifikasi dengan memanfaatkan fasilitas *open Aplication Programing Interface* (API) yang disediakan oleh telegram melalui bot yang dapat digunakan untuk mengirimkan pesan secara otomatis. *Cloud base* pada telegram memungkinkan proses pengiriman jauh lebih cepat serta media penyimpanan yang besar (Fahana dkk, 2017).

2.13 Flowchart

Menurut Indrajani (2011: 22) *Flowchart* merupakan penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program, biasanya mempengaruhi penyelesaian masalah yang khusunya perlu dipelajari dan dievaluasi lebih lanjut.

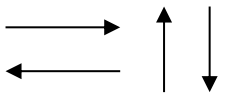
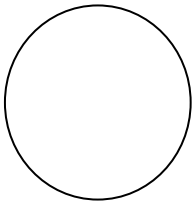
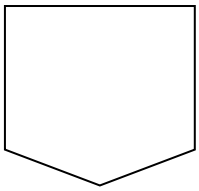
2.13.1 Simbol-Simbol *Flowchart*

Berikut ini merupakan notasi atau simbol-simbol yang digunakan dapat dibagi menjadi tiga kelompok yaitu :

1) *Flow Direction Symbols (*Simbol Penghubung/alur)

Simbol yang digunakan untuk menghubungkan antara simbol yang satu dengan yang lainnya. Simbol ini juga disebut *connecting line*, simbol tersebut adalah :

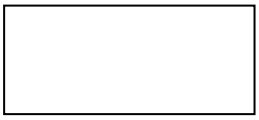
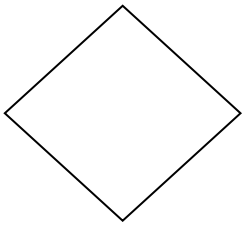
Tabel 2.1 *Flow Direction Symbols (*Simbol Penghubung/alur)

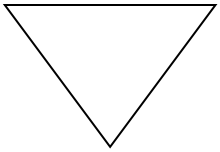
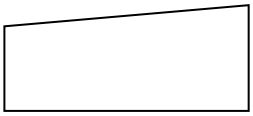
NO	Simbol	Nama	Fungsi
1.		Arus / *Flow*	Untuk menyatakan jalannya arus suatu proses.
2.		*Comunication link*	Untuk menyatakan bahwa adanya transisi suatu data atau informasi dari suatu lokasi ke lokasi lainnya.
3.		*Connector*	Untuk menyatakan sambungan dari satu proses ke proses lainnya dalam halaman atau lembaran sama.
4.		*Offline*	Untuk menyatakan sambungan dari satu proses ke proses lainnya dalam halaman atau lembaran yang berbeda.

2) *Processing Symbols* (Simbol Proses)

Simbol yang menunjukkan jenis operasi pengolahan dalam suatu proses atau prosedur. Simbol-Simbol tersebut adalah :

Tabel 2.2 *Processing Symbols* (Simbol Proses)

NO	Simbol	Nama	Fungsi
1.		Proses	Sebuah fungsi pemrosesan yang dilaksanakan oleh computer.
2.		Manual	Untuk menyatakan suatu tindakan (proses) yang tidak dilakukan oleh komputer (manual).
3.		*Decision* / Logika	Untuk menunjukkan suatu kondisi tertentu, dengan dua kemungkinan, Ya atau Tidak.
4.		*Predefined Process*	Untuk menyatakan penyediaan tempat penyimpanan suatu pengolahan untuk memberi harga awal.
5.		Terminal	Untuk menyatakan permulaan atau akhir suatu program.

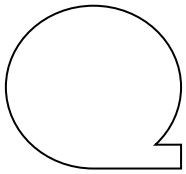
6.		*Offline Storage*	Untuk menunjukkan bahwa data dalam simbol ini akan disimpan ke suatu media tertentu.
7.		Manual *Input*	Untuk memasukkan data secara manual dengan menggunakan *online keyword.*
8.		*Keying Operation*	Untuk menyatakan segala jenis operasi yang diproses dengan menggunakan suatu mesin yang mempunyai *keyboard*.

3) *Input / Output Symbols* (Simbol Masukan / Keluaran)

Simbol yang menunjukkan jenis peralatan yang digunakan sebagai media *input* atau *output.* Simbol – simbol tersebut adalah :

Tabel 2.3 *Input / Output Symbols* (Masukan / Keluaran)

NO	Simbol	Nama	Fungsi
1.		*Input / output*	Untuk menyatakan proses *input* dan *output* tanpa tergantung dengan jenis peralatannya.
2.		*Punched Card*	Untuk menyatakan *input* berasal dari kartu atau output ditulis di kartu.

3.		*Magnetic Tape*	Untuk menyatakan *input* berasal dari pita magnetis atau *output* disimpan ke pita magentis.
4.		*Disk Storage*	Untuk menyatakan *input* berasal dari *disk* atau *output* disimpan ke dalam *disk*.
5.		*Document*	Untuk mencetak keluaran dalam bentuk dokumen (melalui printer).
6.		*Display*	Untuk mencetak keluaran dalam monitor.